

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Michele Steinman, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **5807 Mahon Dr., Columbia, MO 65201** (hereinafter the “**Subject Premises**”) further described in Attachment A, for the things described in Attachment B.

2. I am employed as a United States Postal Inspector with the United States Postal Inspection Service and have been so employed since February of 2022. My duties as a Postal Inspector include the investigations of mail theft (18 U.S.C. § 1078), bank fraud (18 U.S.C. § 1344), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), identity theft (18 U.S.C. § 1028), aggravated identity theft (18 U.S.C. § 1028A), access device fraud (18 U.S.C. § 1029) and other criminal activities. Prior to becoming a Postal Inspector, I was a Special Agent with the United States Department of Treasury, Internal Revenue Service Criminal Investigation (IRS-CI) for approximately 5 years. Before that, I was employed for 12 years as a Special Agent in the United States Secret Service. In both of these previous federal law enforcement positions, I performed investigations involving violations of state and federal law, including cases involving fraudulent activities.

3. As a result of my training and experience in my current and prior positions, I am familiar with federal criminal laws. My primary duties have been the enforcement of federal laws pertaining to financial fraud, identity theft, tax fraud, cyber-crime and other areas. I have worked

on numerous criminal investigations during my federal law enforcement career, often involving fraud, money laundering and other criminal activities, including being the lead investigative agent. During the course of these investigations, I have planned, led, and participated in the execution of search warrants, arrest warrants, witness and suspect interviews, and surveillances; assisted during judicial proceedings; and performed other duties.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of bank fraud (18 U.S.C. § 1344), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), identity theft (18 U.S.C. § 1028), aggravated identity theft (18 U.S.C. § 1028A), access device fraud (18 U.S.C. § 1029) and conspiracy to commit such offenses, have been committed by CALVIN LEE GRAY (“GRAY”) (aka DUSTIN LEE WHITEHEAD), JOANN HELMS (aka JOANN LOSH), and others, both known and unknown, in this investigation. There is also probable cause to search the premises described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED

6. The location to be searched is:

5807 Mahon Dr., Columbia, MO 65201 (the “Subject Premises”). The building is a one story, single family residence with an attached garage. The **Subject Premises** has reddish colored brick with tan siding. The numbers “5807” are visible on a sign on the garage below the coach light. The **Subject Premises** is described Attachment A. In addition, any vehicles parked on the premises or in the driveway are included in this search warrant for the premises.

PROBABLE CAUSE

A. The Fraud Scheme

7. Beginning in at least May of 2023 and continuing to the present day, several victims have reported to various local police departments that their identities have been compromised, bank accounts had been taken over, funds had been withdrawn from their respective bank accounts, and/or bank or credit card accounts have been opened in their identities that they did not authorize. Some of these victims are elderly and the victims resided in multiple states.

8. In April of 2024, the U.S. Postal Inspection Service (“USPIS”) was notified by Detective Kristi Alsup, Boca Raton, Florida Police Department (“BRPD”), of one such victim. Det. Alsup provided USPIS with information related to this fraud scheme and she stated she had identified one of the suspects as GRAY, who often resided at the **Subject Premises**.

1. Fraud as to PNC Bank Accounts

9. Det. Alsup was investigating a fraud case wherein her elderly victim, Victim G.L., had reported various financial fraudulent activities that had occurred with her bank accounts to

BRPD. On or about December 5, 2023, an unknown suspect(s) opened an online checking account with PNC Bank and transferred approximately \$2,000 from Victim G.L.'s existing PNC Bank account ending in 0335 to the newly opened account ending in 1158. Other unauthorized transfers had also been made using Victim G.L.'s accounts. Her cell phone number had also been compromised around this same time. Victim G.L. and her husband, Victim W.W., were the only authorized users on the accounts. Her husband, Victim W.W., was residing at his residence in Creve Coeur, Missouri. It was later determined that Victim W.W. had been victimized in a similar manner with regards to identity theft and fraudulent accounts and transactions and he had reported same to the Creve Coeur, Missouri Police Department.

10. On or about December 17, 2023, Victim G.L. went to her local PNC Bank branch with her sister to get assistance with these fraudulent transactions. While at their local branch, three fraudulent ATM withdrawals were conducted from Victim G.L.'s PNC bank account ending in 0335 in the DeSoto, MO area. The amounts of the fraudulent transactions were \$700, \$500 and \$203. Det. Alsup determined that the three fraudulent ATM withdrawals were conducted using the ATM card assigned to Victim W.W. for Victim G.L.'s PNC account ending in 0335. Two fraudulent withdrawals occurred at the PNC branch located at 224 S. Main St., DeSoto, Missouri. The third fraudulent withdrawal was conducted at a Phillips 66 gas station ATM located at 3625 Athena School Dr., DeSoto, MO.

11. PNC Bank told Det. Alsup that a replacement ATM card was requested and sent to 711 E. Pratt St. in DeSoto, Missouri. In addition, a replacement PIN was sent to the same address

under separate cover. This address is not legitimately associated with Victims G.L. or W.W. in any way.

12. Based upon available surveillance footage obtained from PNC Bank, Det. Alsup was able to identify the person conducting the fraudulent withdrawals as JOANN HELMS (“HELMS”), who was later determined to be the mother of CALVIN GRAY. HELMS resided at 709 E. Pratt St., DeSoto, Missouri, which was an adjacent residence to 711 E. Pratt St. Det. Alsup later determined that 711 E. Pratt was a vacant residence.

2. Credit Card Fraud

13. In January and February of 2024, Det. Alsup learned of additional fraud with respect to Victim G.L. Det. Alsup was provided with a copy of a statement for the time period of December 15, 2023, to January 14, 2024, for Victim G.L.’s Capital One Quicksilver account ending in 6791. This statement showed Southwest Airlines ticket purchases with the passenger names of JOANN HELMS and CALVIN LEE GRAY.

14. In addition, Det. Alsup learned of three attempts to open credit card accounts in Victim G.L.’s identity that she did not authorize. These included a PNC Bank credit card (December 6, 2023), a MasterCard Black Card (December 7, 2023) and an American Express Platinum Card (December 11, 2023).

15. Det. Alsup was also told that Victim G.L. had been locked out of her Gmail account for quite some time and all verification codes were sent to her 610-613-7100 number, which was also compromised by unknown means.

3. Common IP and Telephone Number

16. In February of 2024, Det. Alsup received records from American Express that related to the declined application referenced earlier. The records showed three declined applications submitted fraudulently using Victim G.L.'s identity information. Of note, the application submitted on December 27, 2023, was submitted from **IP 174.34.8.46** (also referred to as the **subject IP**), which was serviced by Socket Telecom.

17. Det. Alsup then learned of fraud on Victim G.L.'s existing American Express ("AMEX") Gold card that had occurred in South Carolina. Det. Alsup contacted AMEX investigators to inquire about the account take over, hereafter referred to as an "ATO," on Victim G.L.'s existing AMEX Gold card account. ATO is defined as a victim's existing account being compromised and used by a suspect for fraudulent transactions.

18. AMEX investigators located two additional accounts that appeared to be related to Victim G.L.'s AMEX gold; an account ending in 5006 and an account ending 9002. The provisioning¹ records for the account ending 9002 showed the provisioning date of November 6, 2023, with the user input first name as "Calvin Gray" and last name as "Calvin Gray" The phone number associated with this account was **314-591-2776**, which was the same as the AMEX account ending in 5006. The address for both accounts was 711 E. Pratt St., DeSoto, Missouri.

19. Det. Alsup conducted research on phone number **314-591-2776**. Her research revealed ten different identities linked to this phone number (including Victim A.S.). Based on my

¹ Apple Pay provisioning refers to the process of adding a credit, debit or pre-paid card to a user's Apple Wallet to be used as a method of payment.

training and experience, when phone numbers associate to multiple identities within a short time frame, it usually indicates the identities were victims of identity theft/fraud.

20. Det. Alsup then spoke with another elderly victim, Victim A.S., who resided in Rolling Hills, California. Victim A.S.'s cell phone of 561-279-7400 had been captured by AMEX when Victim G.L.'s AMEX Gold card was provisioned for Apple Pay. Victim A.S. told Det. Alsup that he had no association to Missouri or anyone in Missouri.

21. Victim A.S. reported his phone was fraudulently ported and he learned of the identity theft and fraud beginning in October of 2023. Victim A.S. told Det. Alsup he received a Citibank card in the mail with the name CALVIN GRAY on it and he also received a Capital One application in close proximity to the time of the phone call with Det. Alsup. Victim A.S. stated he signed up for LifeLock protection and he recently learned the suspects tried to open a PNC Bank account in his name.

22. Victim A.S. also told Det. Alsup that on November 15, 2023 a male called from **314-591-2776** and left a voice message taunting Victim A.S and stating, "You ain't seen nothing yet." Victim A.S. provided Det. Alsup with a photo from the Caller ID on his phone that showed the number calling as **314-591-2776** with the name listed as "GRAY, CALVIN".

23. Det. Alsup further linked this phone number to multiple identity theft victims and instances of fraud throughout this investigation. Instances where this phone number was linked to this scheme (in addition to the above) include its use in: opening accounts in victims' names, calling Victim A.S., calling into financial institutions to access victim accounts, and the Southwest Airlines ticket purchase and at least one West Elm purchase.

24. The same phone number was provided by GRAY as his number when he legally changed his name in 2020. This number is believed to be used/owned/controlled by CALVIN GRAY.

4. Fraudulent Activity from Myrtle Beach, South Carolina

25. A replacement card was ordered for Victim G.L.'s account ending in 6001 on January 15, 2024, and was sent via FedEx to 101 Ocean Creek Drive, Apt F5, Myrtle Beach, South Carolina 29572.

26. Det. Alsup then conducted research on the mailing address of 101 Ocean Creek Drive, Apt FF5, Myrtle Beach, South Carolina. The address was a resort condo property. She spoke with C.L., who managed the condo for his parents. C.L. confirmed to Det. Alsup that the condo was rented via Airbnb from January 14, 2024, to January 21, 2024, to CALVIN GRAY. C.L. told Det. Alsup that the Airbnb profile picture showed a young male with a Thrasher hoodie. C.L. stated the Airbnb messages he received from CALVIN GRAY stated the title of trip was "vacation with my boyfriend".

27. AMEX investigators provided Det. Alsup with the transaction records for the fraudulent charges conducted on Victim G.L.'s AMEX Gold card account ending in 6001. The transactions included a \$387.60 transaction at Cinzia Spa located in Myrtle Beach, South Carolina, on January 19, 2024; two declined transactions at the spa on January 20, 2024; and a declined charge (\$272.49) at a Target in Myrtle Beach, South Carolina, on January 19, 2024. Det. Alsup contacted Cinzia Spa representatives who stated the appointment was made under the name D.E. The names on the waivers were D.E. and Victim W.W. The phone number for Victim W.W. was listed as **314-591-2776**.

28. Det. Alsup contacted Target investigations to attempt to obtain video surveillance of the declined transaction using Victim G.L.'s AMEX gold card ending in 6001.

29. Det. Alsup later obtained surveillance from Target for the attempted fraudulent transaction on Victim G.L.'s AMEX Gold card ending in 6001 on January 19, 2024 in Myrtle Beach, South Carolina. The records showed the attempted purchase was for a pre-paid Samsung AT&T cell phone and a pre-paid Consumer Cellular cell phone. The surveillance video showed a young male wearing black pants and a white hoodie with short brown hair and a light beard attempt to conduct the transaction by inserting the card into the point-of-sale device. Det. Alsup compared known photographs of CALVIN GRAY with these surveillance images from Target and believed it to be GRAY.

5. Additional Victims and Link to the Subject Premises

30. AMEX provided Det. Alsup with records for other accounts and applications using the identities of other probable identity theft/fraud victims that were associated with the account phone numbers and/or mobile devices on known fraudulent accounts/activity and the previously mentioned addresses in Missouri. These included applications that dated back to August of 2022 and, according to AMEX records, the true individuals did not apply for these accounts. The victims were identified as: Victims C.L., W.C., W.W., D.C., E.C., Re. C., Ra. C., and G.A. Some of these individuals had multiple applications submitted in their names.

31. According to AMEX records, Victim D.C. had applications submitted in his name on July 29, 2023, and August 3, 2023, with the listed address as the **Subject Premises**. In addition, on August 10, 2023, Victim D.C. had another fraudulent application submitted in his name with

the billing address listed as 709 E. Pratt St., DeSoto, Missouri, and the home address listed as the **Subject Premises**.

32. Det. Alsup also obtained records related to a fraudulent Capital One SavorOne account ending in 9432 that was opened using Victim G.L.'s identity on December 18, 2023. Capital One sustained a loss of \$2,246.75 believed to be caused by the fraudulent activity conducted on this account associated with Victim G.L. The account address was listed as the **Subject Premises**. The records showed a \$1,756.75 online West Elm.com transaction on December 21, 2023 and two PayPal transactions for \$245 each on December 31, 2023. A third PayPal transaction for \$545.99 was attempted on January 25, 2024 and was declined. The total attempted transactions were \$2,792.74 with \$2,246.75 in actual loss. A second account application was submitted on December 21, 2023, using Victim G.L.'s identity but was declined.

33. Capital One also provided Det. Alsup with records for other accounts and applications using the identities of other probable identity theft/fraud victims believed to be associated with this scheme. These included applications that dated back to October of 2022. The victims were identified as: Victims W.W., V.R., D.C., E.C., Re. C., C.L., G.S., C.G. #1 and C.G. #2. Some of these individuals had multiple applications submitted in their names and many were also associated with the fraudulent applications submitted to AMEX.

34. Det. Alsup also received records related to Victim G.L.'s JP Morgan Chase ("Chase") Southwest Airlines credit card ending in 3453. This account had been compromised. Chase records revealed a new card was requested on January 30, 2024, to 711 E. Pratt St., DeSoto, Missouri. The shipping address was then changed to the **Subject Premises**. The card was sent via UPS and UPS

tracking showed it was delivered to the **Subject Premises** on January 30, 2024. Records showed a \$353.36 Apple Pay purchase associated with this card on January 30, 2024, at a Best Buy in St. Louis, Missouri. Det. Alsup later received records and surveillance related to this Best Buy purchase and determined the suspect in the surveillance conducting the fraudulent purchase to be JOANN HELMS, GRAY's mother.

35. Det. Alsup requested and received records from Southwest Airlines related to a purchase made against Victim G.L.'s Capital One Quicksilver card. The card holder name was Victim W.W. (with the primary on the Capital One Quicksilver account listed as Victim G.L.). The records revealed the purchase was for two tickets that were booked on December 16, 2023 for travel from St. Louis, MO to Las Vegas, NV. The passengers were listed as CALVIN LEE GRAY and JOANN HELMS, with their respective dates of birth. The phone number listed was **314-591-2776**. HELMS' ticket was re-booked several times on December 16, 2023, the last being at 0844 hours via IP address **174.34.8.46**, the **subject IP** mentioned previously in this affidavit. Det. Alsup noted that the records showed HELMS' flight was marked as a no show, with only CALVIN GRAY showing as traveled to Las Vegas.²

² Det. Alsup noted that a fraudulently opened Capital One SavorOne card opened in Victim G.L.'s identity on December 18, 2023, Victim G.L.'s UBS accounts and the fraudulent online PNC accounts were all accessed from Las Vegas geo-located IP connections on December 17, 18 and 19, 2023. Det. Alsup found the fact that the IP addresses geo-locating to Las Vegas was noteworthy in light of the fact that CALVIN GRAY flew to Las Vegas per the Southwest Airlines records on December 16, 2023, thereby establishing GRAY as a suspect conducting the fraud from Las Vegas, Nevada.

36. Det. Alsup received the video files for a Chase checking account ending in 9114, which had been fraudulently opened online on December 11, 2023 in Victim G.L.'s identity. The December 2023 to January 2024 bank statement listed the address of 711 E Pratt St. in DeSoto, Missouri, and the address on the bank statement for the January to February 2024 time period listed the address of the **Subject Premises**.

6. Recent Retail Fraud

37. On or about May 22, 2024, Det. Alsup contacted me regarding additional fraud with respect to Victim G.L. Det. Alsup stated that Victim G.L.'s existing Capital One Saks Fifth Avenue and Neiman Marcus credit cards had been compromised and fraudulent charges were made on both accounts. Victim G.L.'s cards were reported as fraud on March 30, 2024, and replacement cards were sent to the **Subject Premises**.

38. Between April 26, 2024, and May 12, 2024, numerous fraudulent purchases were attempted with both cards totaling over \$10,800. According to records provided by Capital One to Det. Alsup, these purchases occurred at the Saks in Las Vegas, Nevada (April 16–17, 2024) and St. Louis, Missouri locations (April 26, 2024, and May 2 and 12, 2024). There were additional transactions on May 2 and 5, 2024, with the location showing as La Vergne, Tennessee, but this appears to be a Saks distribution center leading investigators to believe that these were online purchases. There was also a fraudulent purchase at the Neiman Marcus St. Louis location on April 26, 2024.

39. I obtained surveillance images and a transaction receipt for the fraudulent purchase of \$1,081.46 on April 26, 2024, at the Neiman Marcus in St. Louis, Missouri. Upon comparing the

person in the surveillance images to known photographs of GRAY, it appeared the person conducting this fraudulent purchase was in fact GRAY. The transaction receipt provided by Neiman Marcus representatives showed Victim G.L.'s name with the **Subject Premises** listed as the address. The items purchased appeared to be clothing. The receipt and a surveillance image are listed below³.



³ Neiman Marcus representatives told me GRAY appeared to be holding a shopping bag from Saks while conducting the fraudulent transaction at their store. Of note, there were two fraudulent purchases at the Saks in St. Louis using Victim G.L.'s Saks card on the same date as this purchase.

	4/26/2024 2:12 PM
Register	47
Transaction	1128
Store	01007
Employee	269083
NM Transaction Type: POS	
Pants	\$195.00
UPC: 401206361610	
Class: 4, Vendor: 48820, Style: 4144960	
Color: 100244, Size: 102709	
Department: 4447	
Salesperson 1: 269083	
Pants	\$225.00
UPC: 401232066008	
Class: 4, Vendor: 48820, Style: 4229076	
Color: 100380, Size: 102709	
Department: 4447	
Salesperson 1: 269083	
Pants	\$225.00
UPC: 401210514422	
Class: 4, Vendor: 48820, Style: 4229076	
Color: 100134, Size: 102709	
Department: 4447	
Salesperson 1: 269083	
Shirts/Tops	\$195.00
UPC: 401208930029	
Class: 1, Vendor: 48820, Style: 3101575	
Color: 100106, Size: 102557	
Department: 4447	
Salesperson 1: 269083	
Travel Acc.	\$150.00
UPC: 401102138996	
Class: 705, Vendor: 30742, Style: 2877949	
Color: 100106, Size: 109999	
Department: 2037	
Salesperson 1: 269083	
Subtotal	\$990.00
Tax	\$91.46
Total	\$1,081.46
NM Charge Card	\$1,081.46 KU
0000410016280468	
Expiration: 07/28	
Cardholder: LASORDA/GAETANA	
Entry Method: Keyed	
Masked Account Number: 609026XXXXXX0548	
Customer Billing Info:	
Customer # 7000319021	
G [REDACTED] L [REDACTED]	
5807 MAHON DR	
COLUMBIA, MO 65201	
Email: florida2676@gmail.com	
Phone1: 3145765228	

In addition, in the records provided by Capital One to Det. Alsup, the IP address of **174.34.8.46** was captured by Capital One records accessing Victim G.L.'s compromised Saks and Neiman Marcus accounts on May 7, 8, 9, 15 and 16, 2024.

7. Use of Fraudulent Identification Documents

40. Capital One investigators also provided Det. Alsup with additional records related to victims that they believed to be related to Victim G.L. in this same or similar scheme. These records included Victims J.S. from Minnesota and W.C. from Missouri.

41. Det. Alsup stated it appeared GRAY had repeatedly contacted Capital One posing as Victims J.S. and W.C. trying to get the victims' checking accounts unfrozen. During these contacts, GRAY was uploading false identification documents in the victims' names and identities trying to verify him calling in as the respective victim to get the account(s) unlocked. These uploads occurred between July of 2023 and April of 2024.

42. Capital One provided Det. Alsup with the some of the images of the false driver's licenses that were being uploaded. Images of the false licenses are listed below:









43. For reference, the photo used on GRAY's Missouri driver's license is listed below:



44. Capital One provided Det. Alsup with approximately 50 call recordings related to these accounts. Det. Alsup stated most of the recordings appeared to be GRAY posing as Victim W.C. During some of the recordings, GRAY provided the address of the **Subject Premises** as the account address. Of note, Det. Alsup stated that Victim W.C. passed away in September of 2023. However, GRAY continued to call in to Capital One up until April 26, 2024, still trying to access Victim W.C.'s account. This was the same date in which one of the false driver's licenses bearing GRAY's photograph, but the name and identifiers of Victim W.C.. was uploaded.

8. HELM's Statement to Police

45. On or about February 29, 2024, Det. Alsup spoke with DeSoto, Missouri Police Department ("DSPD") Detective Sgt. Steger. Det. Steger told Det. Alsup that DSPD had spoken with GRAY's mother, JOANN HELMS, approximately nine months prior and HELMS informed the police that her son (GRAY) conducts identity theft/fraud.

46. HELMS told DSPD detectives that her son's real/given name was DUSTIN WHITEHEAD but that he had legally changed it to CALVIN GRAY. HELMS agreed to give Det. Steger a written statement. The statement read: "I JOANN HELMS got a Fed-Ex envelope yesterday November 6, 2023, and I gave it (the envelope to my son CALVIN GRAY. Also known as DUSTIN WHITEHEAD, he changed his name because of identity theft 3 years ago. So that's when he started this identity theft on others."

B. Use of IP Address 174.34.8.46

47. As set forth herein, the IP address of **174.34.8.46**, the **subject IP**, was frequently associated with fraudulent account applications, transactions, account access and/or orders. There were times USPS Informed Delivery⁴ accounts were created in the victims' identities and/or accessed from this same IP address. This includes an Informed Delivery account in the name of CALVIN GRAY with the address listed as the **Subject Premises** that was accessed on March 5, 2024, using this same IP address.

48. Det. Alsup received records from Socket Telecom for subscriber information for this IP address related to the access on March 5, 2024, as it was within the retention period Socket Telecom retains subscriber information. The records revealed the subscriber to be D.E.,⁵ with the **Subject Premises** listed as both the billing and service addresses. The service start date was listed as February 22, 2023.

⁴ According the US Postal Service website, USPS Informed Delivery is a free service from USPS that shows one preview images of incoming mail, as well as status updates about their incoming mail and outbound packages.

⁵ Det. Alsup believed that CALVIN GRAY was in a relationship with D.E. due to evidence she discovered during the investigation.

49. Examples of this IP address being used to further and execute the fraud scheme included:

- a. Accessing the Chase checking account ending in 9114 (which had been fraudulently opened online in December of 2023 in Victim G.L.'s identity) ninety-one (91) times between December 11, 2023, and February 24, 2024;
- b. Submitting Capital One application in the name of Victim C.G. #1 on August 5, 2023;
- c. USPS Informed Delivery account activation in the name of Victim W.C. on August 15, 2023;
- d. USPS Informed Delivery account access in the name of CALVIN GRAY with the address listed as the **Subject Premises** on August 15, 2023;
- e. USPS Informed Delivery account access in the name of CALVIN GRAY with the address listed as the 29 Portland Drive in St. Louis, MO on August 15, 2023;
- f. USPS Informed Delivery account activation in the name of Victim L.C. on August 30, 2023, and subsequent access on September 1 and 6, 2023;
- g. West Elm order in the amount of \$2,782.52, paid for via the third party finance company Affirm, with the shipping address as CALVIN GRAY at the **Subject Premises** on September 17, 2023;
- h. AMEX account application in the name of Victim G.A. on November 15, 2023;
- i. USPS Informed Delivery account activation in the name of Victim A.S. on November 18, 2023, and subsequent access on November 19 and 23, 2023;

- j. USPS Informed Delivery account access in the name of CALVIN GRAY with the address listed as the **Subject Premises** on August 15, 2023, August 22, 2023, and November 28, 2023;
- k. USPS Informed Delivery account access in the name of CALVIN GRAY with the address listed as 711 E. Pratt St. in DeSoto, Missouri, on November 28 and December 28, 2023;
- l. USPS Informed Delivery account access in the name of Victim W.W. on December 4, 16, and 28, 2023 and on February 4, 2024;
- m. Declined Capital One application in the name of Victim W.W. on December 4, 2023;
- n. UBS financial account access in the name of Victim G.L. on December 11, 15 and 16, 2023;
- o. Purchase of HELMS' Southwest Airlines ticket to Las Vegas, Nevada, on December 16, 2023;
- p. West Elm order in the amount of \$1,756.75 using the fraudulent Capital One SavorOne card ending 9432 in the name of Victim G.L with the shipping address as

Victim W.W. at the **Subject Premises** on December 21, 2023 (order was flagged as fraud and cancelled);

- q. Declined AMEX application in the name of Victim G.L. on December 27, 2023;
- r. Accessing the Regions Bank accounts that were opened online in name of Victim W.W. multiple times in January of 2024;
- s. Accessing HELMS' PNC Bank account on February 26, 2024;
- t. USPS Informed Delivery account access in the name of CALVIN GRAY with the address listed as the **Subject Premises** on August 15, 2023, November 28, 2023, December 28, 2024, and March 5, 2024;
- u. Capital One records accessing Victim G.L.'s compromised Saks and Neiman Marcus credit accounts on May 7, 8, 9, 15 and 16, 2024.

50. As mentioned earlier, Det. Alsup received records from Socket Telecom related to this IP address for the fraudulent use in this scheme on March 5, 2024. These records revealed the service address of **5807 Mahon Dr., Columbia, Missouri**. This same IP address was also captured associated with fraudulent activity on dates before and after March 5, 2024. Based on my training and experience, residential internet IP addresses can often remain static for an extended period and not change.. I believe that the fraudulent activity in which IP address **174.34.8.46** was captured, in all likelihood, was conducted from the same service address of the **Subject Premises**.

C. Probable Cause the Subject Premises Contains Evidence of a Crime

51. Det. Alsup and I documented the address of the **Subject Premises** as it was used or listed multiple times throughout this fraud scheme. Examples of this include:

- a. Socket Telecom records for IP address **174.34.8.46** on March 5, 2024, showing the service address as the **Subject Premises**;
- b. Mailing address for Victim G.L.'s Capital One Quicksilver card was changed to the **Subject Premises**;
- c. Regions Bank accounts in name of Victim W.W. that were opened online in December of 2023 and January of 2024 showing the address as the **Subject Premises**;
- d. Regions Bank credit card accounts in name of Victim W.W. showing the address as the **Subject Premises**;
- e. West Elm order in the amount of \$2,782.52 paid for via the third party finance company Affirm with the shipping address as CALVIN GRAY at the **Subject Premises** on September 17, 2023;
- f. West Elm order in the amount of \$1,756.75 using the fraudulent Capital One SavorOne card ending 9432 in the name of Victim G.L with the shipping address as Victim W.W. at the **Subject Premises** on December 21, 2023 (order was flagged as fraud and cancelled);
- g. West Elm order in the amount of \$2,620.90 paid via Apple Pay with the shipping address as Victim W.W. at the **Subject Premises** on December 21, 2023;
- h. West Elm order in the amount of \$1,196.36 paid via Apple Pay with the shipping address as Victim W.W. at the **Subject Premises** on January 5, 2024;

- i. Victim G.L.'s Capital One Saks and Neiman Marcus replacement cards were sent to the **Subject Premises** on or about March 30, 2024;
 - j. Purchase by GRAY at the Neiman Marcus location in St Louis, Missouri, on April 26, 2024, with transaction receipt showing Victim G.L.'s name with the **Subject Premises** listed as the address;
 - k. Capital One call recordings related to the accounts of Victims J.S. and W.C. Det. Alsup stated most of the recordings appeared to be GRAY posing as Victim W.C. During some of the recordings, GRAY provided the address of the **Subject Premises** as the account address. During some of these calls, false identification documents in the victims' identities were uploaded to Capital One. These uploads occurred multiple times between July of 2023 and April of 2024, with the most recent being on April 26, 2024.
52. In addition, the address of the **Subject Premises** is listed as the "Current Address" on GRAY's Missouri Driver's License.

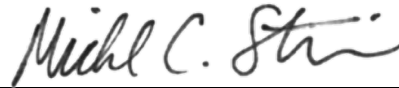
CONCLUSION

Based on the foregoing I submit that this affidavit supports probable cause for a warrant to search the Premises described in Attachment A and seize the items described in Attachment B.

I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature

disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Michele C. Steinman
Postal Inspector
US Postal Inspection Service

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41, on June 4, 2024



THE HONORABLE WILLIE J. EPPS, JR.
CHIEF UNITED STATES MAGISTRATE JUDGE